(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 13/00

(11) 공개번호 특1999-013756
(43) 공개일자 1999년02월25일

(21) 출원번호 특1998-027819
(22) 출원일자 1997년07월26일
(30) 우선권주장 186837 1997년07월11일 일본(JP)
(71) 출원인 가부시끼가이샤도시바 니시무로다이조
일본국 가나가와켄 가와사키시 사이와이구 호리가와쵸 72
(72) 발명자 가또다께히사
일본국 도쿄도 후쮸시 도시바쵸 1 가부시끼가이샤 도시바 후쮸공장 내
(74) 대리인 문기상, 조기호

심사청구 : 있음

(54) 암호화된 카피관리 정보를 갖는 부정 데이터 카피 방지장치 및방법과 기록매체

요약

본 발명은 디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지장치를 개시한다. 상기 디지털 데이터는 암호화된 데이터 본체와, 이 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보를 갖는다. 판정부는 상기 카피관리 정보의 내용이 소정의 조건을 만족하고 있는가의 여부에 의거해서 상기 디지털 데이터가 카피 허가인가의 여부를 판정한다. 금지 처리부는 상기 판정부에 의해 상기 디지털 데이터가 카피 불허가이라고 판정된 경우에는, 상기 디지털 데이터의 유효한 카피 동작을 금지한다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명의 제1 실시예에 관한 부정 데이터 카피 방지장치를 적용하는 디지털 기록 재생기기의 접속 구성례를 나타낸 블록도.

도 2는 상기 실시예에 사용되는 데이터 구조의 구성방법을 설명하는 도면.

도 3은 상기 실시예의 부정 데이터 카피 방지장치에 사용되는 데이터 구조예를 나타낸 도면.

도 4는 상기 실시예의 부정 데이터 카피 방지장치를 사용한 디지털 기록 재생기기의 구성례를 나타낸 도면.

도 5는 상기 실시예의 CF 변경부의 구성 및 그 처리를 나타낸 도면.

도 6은 상기 실시예의 데이터 재생카피 처리부의 구성 및 그 처리를 나타낸 도면.

도 7은 카피관리 플래그(CF)의 구성례를 나타낸 도면.

도 8은 카피 세대의 관리 비트의 상태 천이를 표시한 도면.

도 9는 본 발명의 제2 실시예에 사용되는 데이터 구조의 구성방법을 설명하는 도면.

도 10은 상기 실시예의 부정 데이터 카피 방지장치에 사용되는 다른 데이터 구조예를 나타낸 도면.

도 11은 상기 실시예의 부정 데이터 카피 방지장치의 데이터 재생카피 처리부의 구성 및 그 처리를 나타낸 도면.

도 12는 본 발명의 제3 실시예의 부정 데이터 카피 방지장치에 사용되는 다른 데이터 구조예를 나타낸 도면.

도 13은 본 발명의 제4 실시예예서의 마스터 키 번들(master key bundle)을 이용한 각 기기 사이에서 일시 암호 키를 사용하기 위한 방법을 설명한 도면.

도 14는 상기 실시예의 동작을 설명하는 플로차트.

도 15는 본 발명의 제5 실시예예서의 키 공유회로의 구성례를 나타낸 블록도.

도 16은 키 공유회로에 의해 마스터 키 번들을 사용하지 않고 각 기기 사이에서 일시 암호 키를 공유하기

위한 방법을 설명한 도면.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 부정 데이터 카피 방지장치 및 방법과 기록매체에 관한 것이며, 특히 디지털화된 문서, 음성, 화상, 프로그램 등의 데이터를 부정하게 카피하는 것을 방지하는 부정 데이터 카피 방지장치 및 방법과 기록매체에 관한 것이다.

근년에 디지털 기록 재생기기의 개발, 제품화가 진척되어, 이들 디지털 기록 재생기기 사이에서 화질이나 음질의 열화가 없이 데이터를 카피할 수 있게 되었다.

그러나 열화가 없는 카피가 용이하게 이루어지면, 해적판이라 불려지는 부정한 카피를 증가시켜서 저작권이 침해되는 문제가 있다. 여와 같은 부정한 카피는 확실히 방지하지 않으면 안된다. 왜냐하면 D-VCR나 DVD-RAM 등의 대용량 디지털 기록 재생기기의 출현에 의해 디지털화된 저작물은 간단히 카피되어 불특정 다수에 배포가 가능해지고, 이에 따라 디지털 화상 등의 저작권자에게 위가감을 주고 있기 때문이다.

부정하게 카피하는 수단으로서는 여러 가지 방법을 생각할 수 있으나, 부정자가 부정하게 카피할 때는 DVD-ROM 드라이브나 D-VCR과 같은 재생장치 등의 기기로부터 카피의 대상으로 하는 데이터를 받아서 DVD-RAM 등의 다른 디지털 기록기기로 복사하는 수속을 밟을 필요가 있다.

이와 같은 부정한 데이터 카피를 방지하는 수단으로서, 종래의 DVD 등만큼 대용량이 아닌 디지털 기록 재생기기, 예를 들어 DAT나 MD에서는 SCMS(Serial Copy Management System)라 불려지는 관리 시스템을 사용하고 있다.

SCMS에서는, 예를 들어 CD로부터 MD(또는 DAT)로, 또는 MD(또는 DAT)로부터 MD(또는 DAT)로 데이터를 카피할 때에, 그 데이터 헤드에 카피정보가 부가되어 있다. 이 카피정보는 2비트로 된 데이터로서, 마스터 디스크의 카피정보가 0의 경우에는 카피를 떠도 카피정보는 0 그대로이며, 자유로운 카피가 가능하다.

한편 마스터 디스크의 카피정보가 10의 경우에는 아들 카피(예를 들어 마스터 디스크로부터 1세대 아래 디스크의 카피)는 가능하나, 손자 카피(예를 들어 마스터 디스크로부터 2세대 아래 디스크의 카피)는 불가능하다. 즉 이 경우에는 카피가 이루어지면 이 카피정보가 카운트 업되어 11이 된다. 이것이 아들 카피이다. 그리고 각 시스템은 카피정보가 11의 경우에는 카피할 수 없게 구성되어 있어서, 손자 카피를 방지하도록 되어 있다.

이상의 시스템은 저작권 보호를 위해 부정한 카피를 방지하도록 구성된 정당한 기기를 사용한 경우의 부정 카피 방지방법이다. 그러나 각 기기에 부정 카피 방지의 대책이 마련되어 있어도 기기 사이에서 데이터를 전송할 때에 그 전송로상에서 부정자에 의해 데이터가 부정 유출되어 버린다면, 상기 대책도 무의미한 것이 된다.

이와 같은 데이터 전송시의 부정행위를 방지하기 위해 종래부터 비밀성을 요하는 데이터를 통신할 때에는, 이것을 암호화하여 송신하는 것이 널리 이루어지고 있다. 암호화방식에는 크게 나누어 공개 키방식과 비밀 키방식이 있으나, 상기 경우와 같이 처리의 고속성이 요구될 때에는 비밀 키를 사용하는 것이 일반적이다.

이 비밀 키를 사용하여 암호화를 할 경우에는, 미리 어떤 비밀 키를 사용해서 암호화를 하든가, 통신자간에 정해둔 특정한 비밀 키를 사용해서 암호 통신을 하고 있다.

이 때문에 비밀 키가 제3자에, 예를 들어 공격에 의한 비밀 키의 특정에 따른 도용 등으로 인한 누설이 있으면, 그것이 발각될 경우에 새차 사용하는 비밀 키를 통신자간에 갱신할 필요가 있다. 따라서 보다 유효한 기기간 전송에 있어서의 암호화의 방식이 요망되고 있다.

또 부정한 데이터 카피에 대해서는 이것을 유효하게 재생시키지 못하도록 하는 방법이 필요하다. 또 상기 SCMS에 의한 부정 카피의 관리에서는 아들 카피는 얼마든지 뜰 수 있으므로, 아들 카피로부터의 카피(손자 카피)를 뜰 수는 없어도 악의의 부정자에 의해 아들 카피가 대량으로 작성되는 경우가 있다. 또한 상기한 SCMS에서는 카피정보 자체가 부정자에 의해 예컨대 0으로 기입 변경되면, 이후의 부정 카피는 자유롭게 이루어지게 된다.

따라서 저작권의 문제가 더욱 심각해지는 대용량 디지털 기록 재생기기의 경우에는, SCMS보다도 확실하며 또한 조직적인 카피관리를 실현 가능한 카피관리방법이 요구되고 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 이와 같은 실정을 고려하여 이루어진 것으로서, 그 제1 목적은 데이터 내의 카피관리를 하는 부분에 대한 부정자의 공격을 확실히 방어할 수 있는 부정 데이터 카피 방지장치 및 방법과 기록매체를 제공하는 데 있다.

또 제2 목적은 부정한 카피 데이터를 유효하게 재생시키지 않도록 하는 부정 데이터 카피 방지장치 및 방법을 제공하는 데 있다.

또한 제3 목적은 조직적인 카피관리를 실현 가능한 부정 데이터 카피 방지장치 및 방법을 제공하는 데 있다.

발명의 구성 및 작용

상기의 목적을 달성하기 위해서, 본 발명의 제1 측면은 디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지장치로서,

상기 디지털 데이터는 암호화된 데이터 본체와, 상기 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보를 가지며,

상기 카피관리 정보의 내용이 소정의 조건을 만족하고 있는가의 여부에 의거해서, 상기 디지털 데이터가 카피 허가인가의 여부를 판정하는 판정부와,

상기 판정부에 의해 상기 디지털 데이터가 카피 불허가이라고 판정된 경우에는, 상기 디지털 데이터의 유효한 카피 동작을 금지하는 금지 처리부를 구비한다.

또 본 발명의 제2 측면은 디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지장치로서,

상기 디지털 데이터는 암호화된 데이터 본체와, 상기 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보와, 상기 데이터 본체를 복호하기 위한 키정보를 가지며,

상기 카피관리 정보의 내용이 소정의 조건을 만족하고 있는가의 여부에 의거해서, 상기 디지털 데이터가 카피 허가인가의 여부를 판정하는 판정부와,

상기 판정부에 의해 상기 디지털 데이터가 카피 불허가이라고 판정된 경우에는, 상기 디지털 데이터 내의 상기 키정보를 변경하는 키 변경부를 구비한다.

또 본 발명의 제3 측면은 디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지방법으로서,

상기 디지털 데이터는 암호화된 데이터 본체와, 상기 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보와, 상기 데이터 본체를 복호하기 위한 키정보를 가지며,

상기 카피관리 정보의 내용이 소정의 조건을 만족하고 있는가의 여부에 의거해서, 상기 디지털 데이터가 카피 허가인가의 여부를 판정하는 판정공정과,

상기 판정공정에서 상기 디지털 데이터가 카피 불허가이라고 판정된 경우에는, 상기 디지털 데이터 내의 상기 키정보를 변경하는 키 변경공정을 구비한다.

또 본 발명의 제4 측면은 디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지방법으로서,

상기 디지털 데이터가 최초의 데이터로부터 몇회째의 카피에 상당하는가를 나타내는 세대관리 정보와, 상기 디지털 데이터를 몇회 카피했는가를 나타내는 카피회수관리 정보로 된 카피관리 정보를 상기 디지털 데이터에 부가하는 부가공정과,

상기 세대관리 정보가 소정의 세대수가 되고, 상기 카피회수관리 정보가 소정의 카피회수가 되었을 때, 상기 디지털 데이터에 대한 카피 동작을 금지하는 금지공정을 구비한다.

또 본 발명의 제5 측면은 컴퓨터에 의해 판독 가능한 데이터 구조가 기록된 기록매체로서,

상기 데이터 구조는

암호화된 데이터 본체와,

상기 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보와,

상기 데이터 본체를 복호하기 위한 제1 키정보와,

상기 카피관리 정보를 복호하기 위한 제2 키정보를 구비한다.

또 본 발명의 제6 측면은 컴퓨터에 의해 판독 가능한 데이터 구조가 기록된 기록매체로서,

암호화된 데이터 본체와,

상기 데이터 본체를 복호하기 위한 데이터 암호 키가 상기 데이터 암호 키를 암호 키로 하여 암호화된 제1 키정보와,

상기 데이터 암호 키가 복수의 암호 키에 의해 각각 암호화된 복수의 제2 키정보와,

데이터 본체의 카피 허가에 대해 관리하기 위한 카피관리 정보가 상기 복수의 암호 키에 의해 각각 암호화된 복수의 제3 키정보를 구비한다.

실시예

이하, 본 발명의 실시예에 대해 설명한다.

본 명세서에서는 암호에 관한 기술에 대해 설명하는 데, 이후 암호화의 조작을 Ey(x)로 표시한다. 여기서 x는 암호화의 대상이 되는 데이터이며, y는 암호화에 사용하는 암호 키이다. 또 복호화의 조작을 Dy(z)로 표시한다. 여기서 z는 복호의 대상이 되는 데이터이며, y는 복호화에 사용하는 복호 키이다. 따라서

Ey(Dy(x)) = x

Dy(Ey(x)) = x

이다.

또 본 실시예를 설명하는 도면에서, 1점 쇄선은 암호화 또는 복호화를 위한 키정보를 표시하고, 실선은 암

호화 또는 복호화의 대상이 되는 정보를 표시하고 있다.

(발명의 제1 실시예)

도 1은 본 발명의 제1 실시예에 관한 부정 데이터 카피 방지장치를 적용하는 디지털 기록 재생기기의 접속 구성례를 나타낸 블록도이다.

상기 도면에서는 케이블 텔레비전망을 이용해서 음성/화상/문자 등의 멀티 미디어 정보가 배신(配信)되어 STB(Set Top Box)(101)에 입력되는 예를 나타내고 있다.

이 시스템은 STB(101)가 IEEE1394 케이블(102)을 통해서 디지털 VCR(D-VCR)(103)에 접속됨과 동시에, 디지털 VCR(103)로부터 IEEE1394 케이블(104, 105)을 통해서 각각 디스플레이(106)와 DVD-RAM(107)에 접속되어 구성되어 있다. 상기 시스템에서는 복수의 디지털 기록 재생기기가 접속되어 있으므로, 기본적으로는 기기간에서 데이터 송신, 카피 등이 가능하다.

이 시스템에서는 STB(101), 디지털 VCR(103) 또는 DVD-RAM(107)이 데이터의 송신기기가 되는 것이며, 한편 디지털 VCR(103) 또는 DVD-RAM(107)이 데이터의 수신기기가 되는 것이다. 본 실시예에서는 이들 각 송신기기, 수신기기간의 부정한 데이터 카피를 방지하는 방법에 대해 설명한다.

이하에 상기한 구성을 보다 상세히 설명한다. 우선 STB(101)는 멀티 미디어 데이터의 스크램블을 푼다거나(또는 deshuffling) 과금정보(課金情報) 등의 축적/송신을 하기 위한 것이다. STB(101)에 입력된 멀티미디어 데이터는 IEEE1394 케이블(102, 104, 105)을 통해서 각 기기(103, 106, 107)에 접속되어 있는 데, IEEE1394는 고속 시리얼 디지털 인터페이스(Serial Digital Interface)로서 IEEE에 의해 제정된 것이다. 이 인터페이스로는 고속 통신이 가능하여 Asynchronous(비동기)와 Isochronous(등시)의 2종류의 데이터 전송을 할 수가 있다. 이 때문에 퍼스널 컴퓨터나 디지털 텔레비전, 디지털 VCR, DVD-RAM 등의 디지털 AV기기와의 접속에 이용되는 것이다.

다음에 본 실시예의 부정 데이터 카피 방지방법을 실현하기 위한 데이터 구조에 대해 설명한다.

도 2는 본 실시예에 사용되는 데이터 구조의 구성방법을 설명하는 도면이다.

DVD 등에 저장되는 데이터는 타이틀 키나 디스크 키를 사용해서 내용물(contents)을 암호화한다. 본 실시예에서는 간단하게 하기 위해 내용물은 디스크 키라 불려지는 데이터 암호 키(Dk)로 암호화되는 것으로 한다. 도 2에서 암호화회로(204)에 의해 데이터가 데이터 암호 키(Dk)로 암호화되어 EDk(데이터)가 된 모양을 나타내고 있다. 이 데이터 암호 키(Dk)는 사전에 디지털 기록 재생기기 제조 메이커에 알려지는 일은 없다.

또 디지털 기록 재생기기에서 화상 등의 데이터를 재생하기 위해 상기 데이터 암호 키(Dk)가 암호화되어 데이터 구조의 일부로서 부가된다. 이 암호화된 데이터 암호 키(Dk)는 2종류가 준비된다. 그 하나는 데이터 암호 키(Dk) 자체를 암호 키로 하여 데이터 암호 키(Dk)를 암호화하는 것으로서, 암호화회로(203)에 의해 상기 암호화되어 EDk(Dk)가 된다. 또 하나는 데이터 암호 키(Dk)를 마스터 키 번들(Mkn)의 각 마스터 키로 각각 암호화하는 경우이며, 암호화회로(202)에 의해 키 번들의 키의 수만큼 암호화 데이터 EMk1(Dk), EMk2(Dk), …, EMkn(Dk)가 생성된다.

이 마스터 키 번들(Mkn)은, 예를 들어 키 관리회사에 의해 관리되는 것이며, 디지털 기록 재생기기 제조 메이커는 이 키 관리회사로부터 마스터 키 번들(Mkn)의 일부분인 마스터 키 번들(Mks)이 주어진다. 이 마스터 키 번들(Mks)은 메이커에 따라 다른 복수개의 마스터 키로 되며, 이것에 의해 키관리가 이루어지게 된다. 즉 각 메이커는 마스터 키(Mk1, Mk2, …, Mkn) 중의 적어도 그 일부를 소유하고 있으므로, 데이터 구조 중에 암호화 데이터 EMk1(Dk), EMk2(Dk), …, EMkn(Dk)와 EDk(Dk)가 포함되어 있으면, 데이터 암호 키(Dk)의 인출방법의 상세는 후술한다.

또한 본 발명에서는 데이터 카피를 안전하게 관리하기 위하여 데이터 구조 중에 카피관리 플래그(CF)를 암호화해서 포함시키도록 하고 있다. 즉 도 2에는 카피관리 플래그(CF)가 마스터 키 번들(Mkn)에 의해 암호화회로(201)에서 암호화되어 암호화열 EMk1(CF), EMk2(CF), …, EMkn(CF)이 생성되는 모양이 나타나 있다.

도 3은 본 실시예의 부정 데이터 카피 방지장치에 사용되는 데이터 구조예를 나타낸 도면이다.

상기 도면에는 도 2에 설명한 각 암호화 데이터가 조합되어 데이터 구조를 이루는 모양이 나타나 있다. 즉 각 마스터 키로 암호화된 카피관리 플래그(CF)와 데이터 암호 키(Dk)의 페어(211)가 차례로 정렬되어 마스터 키 암호화부(212)가 구성되고, 마스터 키 암호화부(212)의 뒤쪽에 EDk(Dk)인 디스크 키 암호화부(213)가 부가되어 있다. 그리고 디스크 키 암호화부(213)의 뒤쪽에 EDk(데이터)인 데이터 본체(214)가 형성되어 데이터 구조체(215)를 구성하고 있다.

또한 상기한 바와 같이 데이터 본체(214)는 디지털화된 문서, 음성, 화상 또는 프로그램 등의 데이터가 암호화된 것이며, 이 데이터 본체(214)에 데이터 암호 키(Dk) 및 카피관리 플래그(CF)가 포함된 데이터 구조체(215)가 그대로 또는 더 가공된 형태로 DVD-RAM(107)이나 D-VCR에 기억되고, 또 네트워크 등을 통해서 STB(101)에 송출된다. 즉 이 데이터 구조체(215)의 형태로 송신하거나 기록매체에 기록함으로써 유저에 배포, 판매한다.

그리고 본 발명은 이 데이터 구조체(215)에 포함되어 있는 CF, 즉 암호화되어 외부로부터의 공격에 견딜 수 있는 카피관리 플래그(CF)를 이용해서 데이터의 카피관리(세대관리, 복사회수관리)를 하여, 부정한 카피 데이터를 유효하게 재생시키지 못 하도록 하는 것이다.

이하, 상기 데이터 구조체(215)를 취급하는 디지털 기록 재생기기에 있어서, 어떻게 해서 데이터 재생, 데이터 카피 등을 하는가를 구체적으로 설명한다.

도 4는 본 실시예의 부정 데이터 카피 방지장치를 사용한 디지털 기록 재생기기의 구성례를 나타낸 도면이다.

상기 도면은 송신기기(301)로서 DVD-RAM, 수신기기(302)로서 D-VCR를 사용하고, 양 기기(301, 302)를 IEEE1394 케이블(303)로 접속한 경우를 예로 들어 설명한 것이다. 설명의 편의상, 송신기기(301), 수신기기(302)에는 송신 수신용의 구성만을 나타내나, 각 기기에는 송신 수신용의 양 구성이 포함되어 있다. 또 송신기기(301), 수신기기(302)로서는 도 1에 나타낸 바와 같이 여러 가지 조합을 생각할 수 있다.

송신기기(301)는 IEEE1394 칩(311)과 기록매체인 DVD-RAM(312)로부터 데이터 구조체(215)의 형태로 보존되는 데이터를 판독하고, 또 데이터를 기입하는 판독기입회로(313)로 구성되어 있다. 또한 IEEE1394 칩(311)에는 IEEE1394 인터페이스 처리를 하여 수신기기(302)와 통신하는 IEEE1394 I/F부(314)와, 키 공유회로(315), 암호화회로(316), CF 변경부(317)가 설치되어 있다.

한편 수신기기(302)는 IEEE1394 칩(321, 322)과 대생 데이터에 화질 조정 등을 실시하여 IEEE1394 칩(322)을 통해서 디스플레이(304)로 표시하게 하는 표시 처리부(323)와, IEEE1394 칩(321)의 데이터 재생카피 처리부(334)로부터 출력되는 데이터 구조체(215)를 DV 카세트(324)로부터 데이터 구조체(215)를 판독하여 데이터 재생카피 처리부(334)에 입력하는 판독 처리부(326)로 구성되어 있다. IEEE1394 칩(321)에는 IEEE1394 인터페이스 처리를 하여 송신기기와 통신하는 IEEE1394 I/F부(331)와, 키 공유회로(332), 복호화회로(333), 데이터 재생카피 처리부(334)가 설치되어 있다.

상기 각 구성 중에서 키 공유회로(315, 332)와, 암호화회로(316)와 복호화회로(333)는 데이터 구조체(215)를 IEEE1394 케이블(303)상으로 전송시킬 때에, 이것을 암호화시키 위한 구성이다.

키 공유회로(315, 332)는 IEEE1394 케이블(303)상의 정보 전송에 의해 일시 키(Stk)를 안전하게 공유하도록 되어 있다. 또 암호화회로(316)는 CF 변경부(317)로부터 출력된 DVD-RAM 데이터(데이터 구조체(215))를 키 공유회로(315)로부터의 일시 키(Stk)를 사용해서 암호화한다. 또한 복호화회로(333)는 키 공유회로(332)로부터의 일시 키(Stk)를 사용해서 IEEE1394 I/F부(331)로부터 받은 암호화된 데이터 구조체(215)를 복호하여 데이터 재생카피 처리부(334)에 인도하는 것이다. 그리고 일시 키(Stk)의 키 공유방식에 대해서는 제4 및 제5 실시예서도 상세하게 설명한다.

송신기기(301)의 CF 변경부(317)는 판독기입회로(313)로 판독된 데이터 구조체(215)를 암호화회로(316)에 인도함과 동시에, 카피관리 플래그(CF)를 변경하여 그 CF가 변경된 새로운 데이터 구조체(215)를 가지고 DVD-RAM(312) 내의 동일 데이터 구조체를 갱신한다.

수신기기(302)의 데이터 재생카피 처리부(334)는 복호화회로(333) 또는 판독 처리부(326)로부터 받은 데이터 구조체(215)를 자기가 가지고 있는 키 번들(Mks)에 의해 해독하여 데이터 암호 키(Dk) 및 카피관리 플래그(CF)를 인출함과 동시에, 데이터 암호가 풀린 데이터를 표시 처리부(323)에 출력한다. 또 카피관리 플래그(CF)를 변경한 후, 자기의 마스터 키 번들(Mks)을 사용해서 데이터 구조체(215)를 작성하여, 기입처리부(325)에 보존용 데이터(카피 데이터)로서 출력한다.

다음에 이상과 같이 구성된 본 발명의 실시예에 의한 부정 데이터 카피 방지장치의 동작에 대해 설명한다.

송수신간에서 데이터 전송이 이루어지게 되면, 우선 송신기기(301)와 수신기기(302) 사이에서 키 공유회로(315, 332)에 의해 일시 키(Stk)의 공유화가 이루어진다.

다음에 DVD-RAM(312)으로부터 데이터 구조체(215)가 판독되어 CF 변경부(317)를 통해서 암호화회로(316)에 입력되고, 여기서 데이터 구조체(215)의 일시 키(Stk)에 의한 암호화가 이루어진다. 그리고 암호화된 데이터 구조체(215)는 IEEE1394 I/F부(314)에 의해 IEEE1394 케이블(303)를 통해서 수신기기(302)에 송신된다.

한편 CF 변경부(317)에서는 카피관리 플래그(CF)의 변경이 이루어진다.

도 5는 본 실시예의 CF 변경부(317)의 구성 및 그 처리를 나타낸 도면이다.

상기 도면에 나타낸 바와 같이 DVD-RAM(312)으로부터 판독된 데이터 구조체(215)는 암호화회로(316)에 송출됨과 동시에, 데이터판독 제어회로(401)에 입력된다.

데이터판독 제어회로(401)는 받은 데이터 구조체(215)를

EMk1(Dk), EMk2(Dk), …, EMkn(Dk) …215a

EMk1(CF), EMk2(CF), …, EMkn(CF) …215b

EDk(Dk) : 디스크 키 암호화부 …213

EDk(데이터) : 데이터 본체 …214

로 나누게 되어 있다. EDk(데이터) 이외는 길이가 정해져 있어서, 도 3과 같이 헤더로서 부가된 부분을 나누기가 용이해진다.

그런데 마스터 키 번들(Mkn) 또는 마스터 키 번들(Mks)을 암호 키로 하여 암호화된 데이터 암호 키(215a)는 도 3의 마스터 키 암호화부(212)의 일부이며, 안전을 위해 IEEE1394 칩의 이용자가 마음대로 인출할 수 없는 영역에 기억된다. 이 마스터 키 번들로 암호화된 데이터 암호 키(215a)는 이 장치 제조 메이커에 공급되어 있는 마스터 키 번들(Mks)을 차례로 복호 키로서 사용하여 복호된다.

이 때 EMk1(Dk), EMk2(Dk), …, EMkn(Dk)(215a)는 일단 메모리(402)에 래치되어 제어신호 1로 수신기기의 IEEE1394 칩 내의 마스터 키 번들(Mks)을 차례로 복호 키로서 인출하여 복호화회로(403)에서, 예를 들어 EMk1(Dk)로부터 차례로 복호해간다.

복호하여 얻어진 Dk'를 복호 키로 하여 EDk(Dk)를 복호화회로(404)로 복호하여 Dk를 얻는다. Dk'와 Dk를 판정회로(405)로 비교한다. Dk' = Dk이면, 데이터 암호 키를 암호화하는 데 사용한 마스터 키와 암호화된 데이터 암호 키를 복호하는 데 사용한 마스터 키가 같다는 것과 다름없다. 그러나 Dk' ≠ Dk이면, 데이터 암호 키를 암호화하는 데 사용한 마스터 키와 암호화된 데이터 암호 키를 복호화하는 데 사용한 마스터 키

가 다르다는 것이 된다. 그리고 모든 마스터 키에 대해 Dk' ≠ Dk이면, 이 암호, 예를 들어 EMk1(Dk)는 이 칩이 소유하는 마스터 키 번들(Mks)로는 풀수 없다는 것이 된다.

이와 같은 경우에는 제어신호 2에 의해 다음의 EMk2(Dk)를 메모리(402)로부터 호출하여, IEEE1394 칩 내의 마스터 키 번들(Mks)을 사용해서 상기와 같은 조작을 Dk' = Dk가 되는 EMki가 발견될 때까지 반복한다.

Dk' = Dk가 되면, 그 때의 마스터 키로 EMki(Dk)로부터 데이터 암호 키(Dk)를 인출하게 된다. 그래서 제어신호 3에 의해 메모리(406)에 기억되어 있는 EMk1(CF), EMk2(CF), …, EMkn(CF) 중에서 EMki(CF)를 인출한다. 또한 마스터 키 번들로 암호화된 카피관리 플래그(215b)는 1로부터 n(또는 s)까지 마스터 키 번들로 암호화된 데이터 암호 키(215a)와 같은 열로 되어 있으므로, EMki(CF)의 특정은 용이하다.

다음에 복호화회로(407)에 의해 특정된 마스터 키를 사용한 EMki(CF)의 복호가 이루어지서 CF가 얻어진다. 그리고 CF 변경회로(408)로 카피관리 플래그(CF)가 변경되어 데이터 갱신회로(409)의 암호화회로(410)에 입력된다.

이 데이터 갱신회로(409)에는 데이터판독 제어회로로부터 EDk(데이터), 즉 데이터 구조체(215)의 데이터 본체(214)가 입력하게 되어 있다. 한편 Dk, 변경된 CF도 입력하도록 되어 있고, 암호화회로(410)에서 이들이 마스터 키 번들(Mks) 및 데이터 암호 키(Dk)에 의해 암호화되어 데이터 본체(214)의 헤더로서 주어진다.

이 메이커마다의 마스터 키 번들(Mks)로 암호화되고, 또한 변경된 카피관리 플래그(CF)를 갖는 데이터 구조체(215)(Mkn이 Mks가 된 이외에는 도 3과 동일 구조)가 판독기입회로(313)에 출력되고, 이 새로운 데이터 구조체로 DVD-RAM(312)의 대응하는 부분이 갱신된다.

여기서 카피관리 플래그(CF)는 세대관리 정보와 카피회수관리 정보로 되어 있다. 세대관리라 함은 마스터 디스크로부터 아들 카피, 나아가서는 손자 카피를 만드는 것과 같이 신세대를 만들 경우의 카피관리이다. 한편 카피회수관리라 함은 그 데이터 구조체로 몇회 카피하였는가를 관리하는 것이다. 이 경우에 CF 변경부(317)를 통과해서 암호화회로(316)에 인도된 데이터 구조체(215)는 그것을 받는 측에서 세대관리가 이루어지게 되고, 한편 CF 변경부(317)에 의해 DVD-RAM(312)으로 복귀되어 갱신되는 데이터 구조체는 CF 변경회로(408)로 카피회수만이 카운트 업되어 세대의 변경은 이루어지지 않는다. 또한 카운트수가 최대치가 되는 데이터 송출선(수신기기(302))에서 정상적인 데이터 카피를 할 수 없게 된다.

이와 같이 하여 송신기기(301)에서 카피관리가 이루어지는 한편, 수신기기(302)에서도 수신한 데이터 구조체(215)에 대한 카피관리가 이루어진다. 이하, 수신측에서의 처리를 설명한다.

우선 수신기기(302)의 IEEE1394 I/F부(331)로 받은 암호화된 데이터 구조체는 키 공유회로(332)로부터 주어지는 일시 키(Stk)에 의해 복호화회로(333)로 복호되어 데이터 재생카피 처리부(334)에 입력된다.

도 6은 본 실시예의 데이터 재생카피 처리부의 구성 및 그 처리를 나타낸 도면이다.

데이터 재생카피 처리부(334)에 입력되는 데이터 구조체(215)는 우선 데이터판독 제어회로(401)에 입력되어, 도 5의 CF 변경부(317)의 경우와 마찬가지로 나누어진다. 이하, 판정회로(405)로 데이터 암호 키(Dk)가 인출되고, 또한 복호화회로(407)로 카피관리 플래그(CF)가 인출되기 까지는 도 5의 CF 변경부(317)와 마찬가지의 처리가 이루어진다.

다음에 인출된 카피관리 플래그(CF)의 상태가 CF 판정회로(411)로 판정된다. 카피관리 플래그(CF)의 세대관리 및 카피회수관리의 구체적인 내용은 후술한다. 여기서 카피관리 플래그(CF)가 그 이상 카피할 수 없는 세대인가의 여부, 비록 차세대 카피가 허가되는 세대일지라도 그 데이터 구조체의 카피 가능한 최대회수에 달하고 있는가의 여부가 판정됨으로써 카피의 가부가 판단된다. 그리고 CF 판정회로(411)에 의해 카피관리 플래그(CF) 및 카피 가부의 판정결과(제어신호 4)가 키 변경회로(412)에 주어진다.

키 변경회로(412)는 기록 커맨드나 재생 커맨드 또는 그 양쪽이 유저로부터 입력되어 있는 것을 알리는 제어신호 5로 카피관리 플래그(CF)과, 먼저 얻어진 데이터 암호 키(Dk)를 그대로 또는 변경해서 출력하도록 되어 있다.

데이터를 재생하여 단순히 디스플레이(304)에 표시할 경우에는, 데이터 구조체(215)의 데이터 본체(214)인 EDk(데이터)가 복호화회로(413)로 복호화되고 데이터로서 인출되어 표시 처리부(323)에 출력된다. 이 때, 키 변경회로(412)로부터 복호화회로(413)에는 항상 판정회로(405)에서 인출된 데이터 암호 키(Dk)가 복호화 키로서 주어진다. 따라서 정상적인 데이터 암호 키(Dk)가 인출되는 한, 카피관리 플래그(CF)의 상태에 관계없이 데이터 재생만은 정상적으로 이루어진다.

이에 대해 DV 카세트(324)에 데이터를 카피할 경우에는 CF 한정회로(411)에서의 판정결과에 따라 그 처리가 다르게 된다.

우선 카피관리 플래그(CF)가 카피 가능한 상태에 있을 경우에 대해 설명한다. 이 때에는 키 변경회로(412)로부터는 카피관리 플래그(CF)가 CF 변경회로(414)에 입력되고, 한편 데이터 암호 키(Dk)가 암호화 대상 데이터로서 또한 암호화 키로서 카피회로(415)의 암호화회로(416)에 입력된다.

CF 변경회로(414)에서는 세대의 변경이 이루어진다. 즉 카피관리 플래그(CF)의 세대관리 정보가 변경되어 데이터 구조체가 차세대의 것으로 된다. 이 변경된 카피관리 플래그(CF)는 카피회로(415)에 입력된다.

즉 카피회로(415)에는 데이터 구조체의 데이터 본체(214)인 EDk(데이터)가 데이터판독 제어회로(401)로부터 입력되고, 또한 Dk 및 변경된 CF가 마스터 키 번들(Mks) 및 데이터 암호 키(Dk)에 의해 암호화되어 데이터 본체(214)의 헤더로서 주어진다.

이 메이커마다의 마스터 키 번들(Mks)로 암호화되고, 또한 변경된 카피관리 플래그(CF)를 갖는 데이터 구조체(215)(Mkn이 Mks가 된 이외에는 도 3과 같은 구조)가 기입 처리부(325)에 출력되어, DV 카세트(324)에 카피 데이터로서 저장된다. 또한 이 카피 조작으로 마스터 키 번들이 Mkn으로부터 Mks로 되어 있으므로, 이후에 보존된 데이터 구조체(215)는 이 메이커 호환성이 없어져서 마스터 키 번들(Mks)을 갖지 않은 기기

에서는 재생이나 카피를 할 수 없게 된다.

또 이 보존된 데이터 구조체(215)를 재생할 경우에는, 판독 처리부(326)로부터 마스터 키 번들(Mks)로 암호화된 데이터 구조체가 데이터판독 제어회로(401)에 입력되어 상기와 마찬가지 처리가 이루어진다.

다음에 카피관리 플래그(CF)가 카피 가능한 상태에 있지 않을 경우에 대해 설명한다. 이 때 데이터 구조체는 이미 카피할 수 없는 상태에 있으므로, CF 변경회로(414)에서는 특히 카피관리 플래그(CF)의 변경은 하지 않는다. 한편 키 변경회로(412)로부터 암호화회로(416)로의 데이터 암호 키의 출력이 카피 가능한 경우와 다른 것이 된다.

즉 카피가 불가능한 경우에 키 변경회로(412)는 암호화 대상 데이터 그리고 암호화 키가 되는 데이터 암호 키로서 판정회로(405)로 인출된 정규의 데이터 암호 키(Dk)와는 다른 가짜의 데이터 암호 키(Dk*)를 암호화회로(215)에 입력한다. Dk를 변경해서 가짜의 Dk*를 만들기 위해서는, 예를 들어 Dk의 비트를 반전하든가, 비트 시프트를 하든가, 어떤 특정한 수치와의 배타 논리합을 취하는 등의 방법이 있다.

그리고 각 데이터가 주어진 카피회로(415) 및 암호화회로(416)의 처리는 상기와 마찬가지이다. 그러나 이 회로(415)로 생성되어 보존된 데이터 구조체(215)에 있어서는, 도 3의 EDk(데이터)의 암호 키는 Dk 그대로이며, 헤더부인 마스터 키 암호화부(212) 및 디스크 키 암호화부(213)에 사용되어 저장되는 데이터 키(Dk*)는 모두 가짜의 것이 되어 있다. 따라서 이 데이터 구조체를 복호할 때는, 가짜의 데이터 암호 키(Dk*)가 인출되어 가짜의 데이터 암호 키(Dk*)에 의한 엉터리의 데이터 재생이 이루어지게 된다.

이상이 송신기기(301)로부터 수신기기(302)로 데이터 구조체(215)를 카피하고, 또 데이터를 재생할 경우의 처리이다. 즉 송신기기(301)에서 소스 데이터에 대한 데이터 카피의 회수관리가 이루어지고, 수신기기(302)에서 받은 데이터를 카피하는 데이터 카피의 세대관리가 이루어지고 있다.

다음에 카피관리 플래그(CF)의 구체적인 내용 및 세대관리, 카피회수관리에 대해 도 7, 도 8을 사용해서 설명한다.

도 7은 카피관리 플래그(CF)의 구성예를 나타낸 도면이다. 본 실시예에서는 8비트를 1바이트로 하고, 상위 3비트를 카피 세대의 관리를 위한 비트(세대관리 정보)로 하고, 하위 5비트를 카피회수를 관리하기 위한 비트(카피회수관리 정보)로 하고 있다.

도 8은 카피 세대의 관리 비트의 상태 천이를 표시한 도면이다. 카피세대관리 비트는

000 … 카피 가능

001 … 아들 카피 가능(손자 카피는 불가능)

→아들은 111이 된다

011 … 손자 카피 가능(증손 카피는 불가능)

→아들은 001이 되고, 손자는 111이 된다

111 … 카피 불가능

로 된다. 따라서 도 8과 같이 카피세대관리 비트가 전부 0일 경우에는 카피를 하여도 전부 0 그대로이나, 카피세대관리 비트가 1일 경우에는 아들의 카피는 가능하나, 손자의 카피는 불가능하기 때문에 카피 불가능이 된다. 한편 카피세대관리 비트가 11일 경우에는 손자 카피까지 가능하므로, 아들 카피세대관리 비트는 10이 되고 손자 카피의 카피세대관리 비트는 111이 되어 카피 불가능이 된다. 이렇게 하여 카피 세대를 관리하는 것이다.

또 카피회수는 카피회수관리 비트가 최대치가 되면, 비록 카피세대관리 비트가 카피 가능한 세대일지라도 카피 불가능이 된다. 본 실시예에서는 카피회수관리 비트가 5비트이기 때문에 1회로부터 32회까지의 회수관리밖에 할 수 없으나, 비트수를 증가하면 더욱 많은 회수관리가 가능하다.

회수관리의 경우에, 예를 들어 소프트웨어의 마스터 디스크의 유저수를 제한하는 경우 등에 이용 가능하다. 마스터 디스크의 카피세대관리 플래그는 아들의 카피가 가능한 1로 하여 둔다. 이렇게 하면 유저가 카피한 소프트웨어가 거듭 카피되는 것을 방지할 수가 있다.

카피회수관리 비트는 마스터 디스크로부터 카피할 수 있는 유저수를 표시하고 있으며, 본 실시예의 경우에는 0~32명까지 카피할 수가 있다.

예를 들어 마스터 디스크로부터 카피 가능한 유저수를 10명으로 한다. 이 경우에 최초의 카피회수관리 비트는 1010이다. 1명이 카피하면

마스터 디스크의 CF : 00101001

유저의 CF : 11100000

이 되어 유저가 카피한 소프트웨어는 다른 매체에 기록할 수가 없게 된다.

이렇게 하여 10명의 유저가 소프트웨어를 카피하면

마스터 디스크의 CF : 00100000

이 되어 아들 카피는 가능한 채로 있지만, 회수가 0회이기 때문에 그 이상의 카피는 허가되지 않는다.

또한 최후의 사람이 카피한 시점에서 마스터 디스크의 카피세대관리 비트를 111로 해 두는 방법도 있다.

상술한 바와 같이 본 실시예에 관한 부정 데이터 카피 방지장치 및 방법은 카피관리를 하는 부분인 카피관리 플래그(CF)를 암호화하여 데이터 구조체(215)에 포함시키도록 하였으므로, 카피관리 플래그(CF)를 전송도중에 기입 변경하여 부정 카피를 방지할 수 있어서, 카피관리 플래그(CF)에 대한 부정자의 공격을 확실

허 방어할 수 있다. 이에 따라 저작권을 확실히 보호할 수가 있다.

또 데이터 재생카피 처리부(334)에 CF 판정회로(411) 및 키 변경회로(412)를 설치하여 카피할 수 없는 데이터 구조체를 카피할 때에는, 데이터 암호 키를 변경하도록 하였으므로 부정한 카피 데이터를 유효하게 재생시키지 않도록 할 수가 있다. 즉 디지털 데이터가 카피 불허가로 판정되었을 때는 디지털 데이터 내의 키정보가 변경되어, 그 카피된 디지털 데이터는 유효한 재생을 할 수 없게 된다. 이에 따라 디지털 데이터의 유효한 카피 동작이 금지된 것과 마찬가지 효과를 얻을 수가 있다.

또 CF 변경부(317)를 설치하여 카피를 위해 전송하는 데이터 구조체의 카피회수를 카운트 업시킬 수가 있어서, 조직적이고 효과적인 카피관리를 실현할 수가 있다.

또 키 공유회로(315, 332) 및 암호화회로(316)를 설치하여 전송되는 데이터 구조체를 암호화하도록 하였으므로, 수신측에 복호화회로(333)를 갖추고 있지 않으면 당해 데이터를 이용할 수 없도록 할 수가 있다. 또 기기간을 일시적인 암호 키로 암호화해서 전송하기 때문에 기기간을 접속하는 케이블로부터 다른 기록매체에 기록하여 재이용하는 부정한 카피를 방지할 수가 있다.

또한 카피가 가능한가의 여부를 나타내기 위한 카피관리 플래그(CF)에는 카피가 몇 세대까지 가능한가를 나타내는 부분과, 카피회수가 몇회까지 가능한가를 나타낸 부분을 형성하였으므로, 카피의 세대관리와 회수관리에 의해 조직적인 카피 허가불허가관리를 할 수가 있다.

또한 본 실시예에서는 CF 변경부(317), 데이터 재생카피 처리부(334)는 각각 IEEE1394 칩(311, 321)에 포함되는 구성으로 하였으나, 본 발명은 이와 같은 구성에 한정되는 것은 아니며, 예를 들어 CF 변경부(317), 데이터 재생카피 처리부(334)가 별개 칩으로 되는 구성으로 하여도 좋다.

(발명의 제2 실시예)

본 실시예에서는 부정 데이터 카피 방지방법을 실현하기 위한 다른 데이터 구조에 대해 설명한다.

도 9는 본 발명의 제2 실시예에 사용되는 데이터 구조의 구성방법을 설명하는 도면이며, 도 2와 동일 부분에는 동일 부호를 붙여서 설명을 생략한다.

도 9에서는 카피관리 플래그(CF)를 암호화하는 암호화 키에 데이터 암호 키(Dk)가 사용되는 외에는, 각 데이터의 암호화는 제1 실시예와 마찬가지이다. 단 도 2에서는 마스터 키 번들이 사용되는 관계상, CF의 암호화 데이터는 복수로 되었으나, 본 실시예에서는 데이터 암호 키(Dk)가 사용되므로 CF의 암호화 데이터는 하나이다.

도 10은 본 실시예의 부정 데이터 카피 방지장치에 사용되는 다른 데이터 구조의 예를 나타낸 도면이다.

상기 도면에는 도 9에 설명한 각 암호화 데이터가 조합되어 데이터 구조를 이룬 모양이 나타나 있다. 즉 이 데이터 구조체(226)에서는 데이터 암호 키(Dk)로 암호화된 카피관리 플래그(221)와, 마스터 키로 암호화된 데이터 암호 키(222)가 차례로 정렬된 마스터 키 암호화부(223)와 EDk(Dk)인 디스크 키 암호화부(224)가 차례로 정렬된 헤더부로 되어 있다. 그리고 EDk(데이터)인 데이터 본체(225)의 선두에 이 헤더부가 형성되어 데이터 구조체(226)로서 구성되어 있다.

이와 같은 데이터 구조체(226)는 데이터 카피의 카리관리, 부정 카피 방지를 실현하기 위한 부정 데이터 카피 방지장치를 갖춘 디지털 기록 재생기기에서 기록 재생용 데이터로서 사용된다.

그 적용 대상은 제1 실시예에서 설명한 디지털 기록 재생기기와 마찬가지이다. 즉 데이터 구조체(226)는 데이터판독 제어기기에서의 할당 대상이 일부 변경되어 CF를 암호 복호하는 키가 Dk로 되어 있는 외는 도 1, 도 4, 도 5, 도 6에 나타낸 각 장치에서 이용할 수 있다.

또한 데이터 구조체(226)를 사용한 경우의 도 6에 대응한 데이터 재생카피 처리부(334b)의 구성을 도 11에 나타낸다.

도 11은 본 실시예의 부정 데이터 카피 방지장치의 데이터 재생카피 처리부의 구성 및 그 처리를 나타낸 도면이며, 도 6과 동일 부분에는 동일 부호를 붙인다. 그리고 부정 데이터 카피 방지장치를 포함한 시스템의 전체 구성은 도 4에 나타낸 경우와 마찬가지이다.

상기 도면에서 제1 실시예(도 6)와의 상이점은 데이터판독 제어회로(401)에 데이터 구조체(226)가 입력되고, 그 데이터 할당에 의해 EDk(CF)를 메모리(406)에 입력하고 마스터 키 암호화부(223)를 데이터 본체(225)와 더불어 카피회로(415b)에 입력하는 점과, 복호화회로(407)에서 사용되는 복호화 키가 판정회로(415b)에서 얻어지는 데이터 암호 키(Dk)로 되어 있는 점과, 또 카피회로(415a)에서는 각 부로부터의 입력에 의해 데이터 구조체(215)가 아니고 데이터 구조체(226)를 생성하는 점이다. 또한 카피회로(415b)에서는 데이터판독 제어회로(401)로부터 입력된 마스터 키 암호화부(223)가 데이터 구조체(226)의 헤드부의 일부에 그대로 이용된다. 또한 카피 불가능시에 Dk가 Dk*로 변경되었을 경우에, EDk*(Dk*)가 되는 새로운 디스크 키 암호화부(224)의 Dk*가 Dk와 다르게 되어 있으므로, 이 데이터 구조체의 마스터 키 암호화부(223)로부터 데이터 키(Dk)가 인출되는 일은 없다.

그 결과, 카피회로(416)로부터 출력되는 데이터 구조체(226)는 CF가 변경되거나 또는 부정 카피시에 Dk*가 변경되는 외에는, 데이터 재생카피 처리부(334)에 입력된 데이터 구조체(226) 그대로이다. 특히 마스터 키 암호화부(223)가 메이커마다의 마스터 키 번들(Mks)로 치환되는 일은 없으므로, 카피된 데이터는 메이커 호환성을 상실하는 일은 없다.

또한 본 실시예에서 사용되는 송신측의 CF 변경부도 상기 도 6~도 11과 마찬가지 변경이 도 5에 나타낸 CF 변경부(317)에 실시된다(도시하지 않음). 즉 복호화회로(407)에 복호 키로서 데이터 암호 키(Dk)가 입력되고, 데이터 갱신회로(409)에 마스터 키 암호화부(223)가 입력되어 갱신용의 데이터 구조체(226)의 헤드부에 이용된다. 따라서 카피회수관리시에도 데이터 구조체(226)는 메이커 호환성을 상실하지 않는다.

상술한 바와 같이 본 발명의 실시예에 관한 부정 데이터 카피 방지장치 및 방법은 제1 실시예와 마찬가지

로 구성으로 한 외에, 디지털 데이터로서 데이터 구조체(226)를 사용하도록 하였으므로 제1 실시예와 마찬가지 효과가 얻어지는 외에, 데이터를 카피할 때에, 최초의 마스터 키 번들(Mkn)로 암호화된 데이터 암호키를 그대로 넘겨줄 수가 있어서, 카피 데이터나 카피원인 데이터의 데이터 호환성을 상실하지 않도록 할 수가 있다.

(발명의 제3 실시예)

제1 또는 제2 실시예에서는 도 3에 나타낸 데이터 구조체(215) 또는 도 10에 나타낸 데이터 구조체(226)만이 시스템에 사용되는 경우에 대해 설명하였다. 그러나 실제의 사용에서는 이들 각 데이터 구조체가 혼재하는 경우도 생각할 수 있다. 본 실시예에서는 이와 같은 경우의 대응방법에 대해 설명한다.

도 12a, 도 12b는 본 발명의 제3 실시예의 부정 데이터 카피 방지장치에 사용되고 있는 다른 데이터 구조체를 나타낸 도면이다.

12A는 데이터 구조체(215)의 선두에 식별 비트(231a)를 부가하여 데이터 구조체(215b)로 한 것을 나타낸다.

한편 도 12b는 구조체(226)의 선두에 식별 비트(231b)를 부가하여 데이터 구조체(226b)로 한 것을 나타낸다.

데이터 재생카피 처리부(334, 334b), CF 변경부(317)(제2 실시예의 경우를 포함한다)의 데이터판독 제어회로(401)는 이 식별 비트(231a, 231b)를 판독하여 각 부에 어느 데이터 구조체에 대응한 처리를 할 것인가의 제어신호를 출력한다.

상술한 바와 같이 본 발명의 실시예에 관한 부정 데이터 카피 방지장치 및 방법은 제1 또는 제2 실시예와 마찬가지 구성으로 한 외에, 디지털 데이터로서 데이터 구조체(215b, 226b)를 사용하도록 하였으므로 제1 또는 제2 실시예와 마찬가지 효과가 얻어지는 외에, 상이한 형식의 데이터 구조체를 혼재시켜도 각각의 데이터 구조에 대응한 처리를 할 수가 있다.

(발명의 제4 실시예)

상기 각 실시예에서는 데이터 구조체를 어떠한 구성으로 하고, 이것에 포함되는 카피관리 플래그(CF)에 의해 어떻게 데이터 카피관리를 하는가에 대해 설명하였다. 그러나 상기 방법으로 데이터 카피관리를 하여도 데이터 전송상에서 데이터 구조체를 부정으로 취득 당하여, 소위 부정 유출되어버리면 상기 데이터 관리방법의 효과도 감소하게 된다. 이를 방지하기 위해 상기 각 실시예에서는 키 공유회로(315, 332)를 설치하여 일시 키(Stk)를 공유하고, 이 일시 키(Stk)로 암호화된 데이터를 전송로(IEEE1394 케이블(303))상에서 전송시키도록 하고 있다.

본 실시예 및 제5 실시예에서는 이 일시 키(Stk)를 공유하는 방법에 대해 설명한다. 따라서 본 실시예 및 제5 실시예로 이하에 설명되는 키 공유 시스템이 제1, 제2 또는 제3 실시예의 키 공유회로(315, 332)에 사용하게 된다.

도 13은 본 발명의 제4 실시예에서의 마스터 키 번들을 이용한 각 기기간에서 일시 키를 공유하기 위한 방법을 설명한 도면이며, 네트워크 또는 케이블에 의해 접속된 기기간에서 네트워크 또는 케이블상을 흐르는 비밀정보를 암호화/복호화하기 위한 일시 키의 공유방법에 대해 도시한 것이다. 본 실시예에서는 IEEE1394로 접속된 송신기기와 수신기기 사이에서 일시 키를 공유하는 경우에 대해 설명한다.

상기 도면에서 송신기기(501)와 수신기기(503)가 IEEE1394 케이블(303)에 의해 접속되어 있다. 송신기기에 마스터 키의 키 번들(504a)(Mks)이 기록되고, 수신기기에 마스터 키의 키 번들(504b)(Mks)이 기록되어 있다. 양자의 키 번들은 달라도 상관 없으나, 반드시 키 번들 두의 몇 개인가는 같은 마스터 키가 포함되어 있을 필요가 있다. 본 실시예에서는 양자의 마스터 키의 키 번들(Mks)은 같은 것으로 한다.

송신기기(501)의 키 공유에 관한 부분은 일시 키 생성회로(505)와 암호화회로(507a, 507b)로 구성된다.

일시 키 생성회로(505)는 네트워크 또는 케이블상을 흐르는 데이터를 일시적으로 암호화하기 위한 일시 키를 생성하는 것이다. 이 일시 키 생성회로(505)는, 예를 들어 특정한 길이의 난수를 생성하는 난수 발생기로 하는 것이 바람직하다.

일시 키(506)(Sk)는 일시 키 생성회로(505)로 생성된 키이다.

암호화회로(507a)는 마스터 키의 키 번들(504a)의 어느 것인가로 일시 키(506)를 암호화하는 회로이고, 암호화회로(507b)는 일시 키(Sk)를 일시 키(Stk)로 암호화하는 회로이다. 암호화회로(507a)와 암호화회로(507b)는 암호화방식이 같으면, 동일한 회로이어도 상관이 없다. EMki(Sk)(508)는 암호화회로(507a)의 출력이고, ESk(Sk)(509)는 암호화회로(507b)의 출력이다.

한편 수신기기(503)의 키 공유에 관한 부분은 복호화회로(510a, 510b)와 일시 키 판정회로(513)으로 구성된다.

복호화회로(510a)는 암호화회로(507a)의 출력을 마스터 키의 키 번들(Mki)로 복호한다. 복호화회로(510b)는 암호화회로(507a)의 출력을 복호화회로(510a)의 출력으로 복호한다.

Ska(511)는 복호화회로(510a)의 출력이고, Skb(512)는 복호화회로(510b)의 출력이다.

일시 키 판정회로(513)는 복호화회로(510a)의 출력과 복호화회로(510b)의 출력을 비교 판정하는 판정회로이다. 제어신호(514)는 판정의 결과에 따라 마스터 키의 키 번들을 변경하기 위한 신호이며, Sk(515)는 판정의 결과로 얻어진 일시 키이다.

다음에 이상과 같이 구성된 본 발명의 실시예에 관한 일시 키 공유장치의 동작에 대해 설명한다.

우선, 만일 마스터 키가 1개만 존재한다고 하면(이것을 Mk0라 한다), 단순히 송신기기(501)에서 Mk0로 Sk를 암호화하고, 이 EMk(Sk)를 수신기기(503)에 보내어, 수신기기(503)에서 Mk0로 EMk(Sk)를 복호화함으로써

Sk를 인출할 수가 있다. 그러나 만일 마스터 키가 파괴된(누설된) 경우에는 마스터 키를 교환하지 않으면 안되며, 새로운 기기와 오래 된 기기 사이에 호환성이 없게 될 가능성이 있다.

따라서 본 실시예에서는 복수의 마스터 키로 된 번들(Mks) 중에서 사용한 마스터 키(Mki)를 직접적으로 지정하여 나타내는 식별정보는 송신기기(501)로부터 수신기기(503)에는 보내지 않고, 그 대신에 상기 마스터 키(Mki)를 특정 가능하게 하는 정보(여기서는 EMki(508) 및 ESk(Sk)(509)를 의미한다)를 송신기기(501)로부터 수신기기(503)에 보내어, 수신기기(503)에서 Sk의 암호화에 사용된 마스터 키(Mki)가 마스터 키 중의 어느 것인기를 특정함과 동시에, 이 마스터 키의 특정을 통해서 Sk를 얻는다.

도 14는 본 실시예의 동작을 설명하는 플로차트이다.

우선, 송신기기(501)에서 수신기기(503)와의 사이에서 공유되는 일시 키(506)가 일시 키 생성회로(505)로 생성된다(S11).

이하, 도 14의 스텝(S12)의 보다 상세한 절차에 대해 설명한다.

생성된 Sk는 n개의 마스터 키(공통 키 암호방식에서의 공통 키)의 키 번들(504a) 중으로부터 예컨대 랜덤 또는 차례로 선택한 1개(이것을 Mki로 한다)로 암호화된다. 즉 Mks(s = 1, …, n ; n은 2 이상의 정수) 중의 어느 1개의 Mki로 일시 키(Sk)를 암호화회로(507a)에서 암호화하여 EMki(Sk)를 얻는다.

이 마스터 키(Mks)는 미리 등록되어 있는 것이며, 유저는 볼 수 없는 방법으로 되어 있다. 그리고 만일 마스터 키가 파괴된 것이 발각되었을 경우는, 그 이후에 송신기기에는 그 파괴된 것을 제외한 마스터 키가 제작 삽입된다. 수신기기(503)측은 그 파괴된 것을 제외한 마스터 키가 제작 삽입되어도 좋고, 그렇지 않아도 좋다. 단 IEEE1394의 경우에는, 어느 기기가 송신기기가 되느냐 수신기기가 되느냐의 구별이 없기(D-VCR이나 DVD-RAM 등의 녹화 재생기기는 송신기기와 수신기기가 될 수 있다) 때문에 파괴된 마스터 키를 제외한 것으로 바꾸는 것이 바람직하다. 또한 전체의 제어는 도시하지 않은 각 기기 내의 제어부가 관장하는 것으로 한다. 제어부는, 예를 들어 프로그램을 각 기기 내에 내장된 CPU 등으로 실행함으로써 실현할 수가 있다.

또한 암호화회로(507b)에 의해 Sk 자체를 암호 키로 사용하여 Sk를 암호화해서 ESk(Sk)를 얻는다. 그리고 EMki(Sk)와 ESk(Sk)를 IEEE1394 케이블(502)을 통해서 수신기기(503)에 보낸다.

또한 수신기기(503)로 우선 마스터 키를 1개 선택한다(이것을 Mkp로 한다). 선택한 Mkp를 복호 키로 하여 복호화회로(510a)에 의해 복호화하고

DMkp(EMki(Sk)) = Ska

를 얻는다.

다음에 복호화회로(510a)로부터의 출력(Ska)을 복호 키로 하여 복호화회로(510b)에 의해 ESk(Sk)를 복호화하고

DSka(ESk(Sk)) = Skb

를 얻는다.

다음에 일시 키 판정회로(513)에 의해 Ska와 Skb가 일치하는가의 여부를 조사한다. 여기서 송신기기(501)로 Sk를 암호화한 마스터 키(Mki)기 마스터 키 (Mkp)이면

Ska = DMkp(EMki(Sk)) = Sk

가 되고, 따라서

Skb = DSka(ESk(Sk)) = DSk(ESk(Sk)) = Sk

가 되며, 고로

Ska = Skb = Sk

가 된다.

즉 일시 키 판정회로(513)에 의해 Ska와 Skb가 일치하는 것을 알 경우에는

Mki = Mkp, 또한 Ska = Skb = Sk

이며, 이 경우에 일시 키 판정회로(513)는

Ska = Skb = Sk

를 출력한다.

한편 일시 키 판정회로(513)에 의해 Ska와 Skb가 일치하지 않은 것을 알 경우에는

Mki ≠ Mkp

이고, 송신기기(501)에서 Sk는 이 Mkp로 암호화된 것이 아니므로, 그 이외의 마스터 키로 암호화된 것을 알 수 있다. 이 경우에 일시 키 판정회로(513)는 출력을 하지 않거나, 또는 일시 키 판정회로(513)의 출력은 이후의 처리부로 전달되지 않는다.

이후는 Ska와 Skb가 일치할 때까지 복호화에 사용하는 Mkp를 변경하여 상기 절차를 반복한다. 예를 들어 최초에 Mkp와 Mk1을 사용하여 상기한 절차를 밟아서 Ska와 Skb가 일치하지 않을 경우에는, 다음에 Mk2로 갱신하여 다시 상기한 절차를 반복하는 것이다.

이상과 같은 절차를 사용하여 송신기기(501)에서 어느 마스터 키를 사용했는가를 수신기기(503)에서 특정

할 수 있음과 동시에, 송신기기(501)와 수신기기(503) 사이에서 일시 키(Sk)를 안전하게 공유할 수 있게 된다.

상술한 바와 같이 본 발명의 실시예에 관한 부정 데이터 카피 방지장치 및 방법은 제1, 제2 또는 제3 실시예와 마찬가지 구성으로 한 외에, 마스터 키를 사용하여 송신기기(501)와 수신기기(503) 사이에서 일시 키(Sk)를 안전하게 공유할 수 있게 하였으므로, 제1, 제2 또는 제3 실시예와 마찬가지 효과가 얻어지는 외에, 기기간을 접속하는 케이블로부터 다른 기록매체로 기록하여 재이용하는 부정한 카피를 보다 한층 확실히 방지할 수가 있다.

(발명의 제5 실시예)

본 실시예에서는 일시 키를 공유하는 다른 방법, 즉 마스터 키를 사용하지 않고 일시 키를 공유하는 방법에 대해 도 15와 도 16을 사용하여 설명한다.

이 방식은 니께이 일렉트로닉스 No. 676, pp. 13-14, 1996. 11. 18에 개시된 기술을 응용한 것이다.

도 15는 본 발명의 제5 실시예에서의 키 공유회로의 구성례를 나타낸 블록도이다.

도 16은 이 키 공유회로에 의해 마스터 키 번들을 사용하지 않고 각 기기간에서 일시 암호 키를 공유하기 위한 방법을 설명한 도면이다.

지금 IEEE1394로 접속된 기기에 노드가 할당되고, 도 16에 나타낸 바와 같이 노드 #1과 노드 #2로 일시 키를 공유하는 것으로 한다. 우선 도 15를 사용하여 본 실시예에서의 키 공유 절차에 사용하는 키 공유회로(630a, 630b)의 구성에 대해 설명한다.

키 공유회로(630a)는 챌린지 키 생성회로(631a), 인증 키 생성회로(633a), 비교회로(635a), 일시 키 생성회로(637a)를 갖추고 있다.

마찬가지로 키 공유회로(630b)는 챌린지 키 생성회로(631b), 인증 키 생성회로(633b), 비교회로(635b), 일시 키 생성회로(637b)를 갖추고 있다.

챌린지 키 생성회로(631a, 631b)는, 예를 들어 난수 생성 알고리즘을 사용하여 생성할 때마다 변화하는 챌린지 키를 생성한다.

인증 키 생성회로(633a, 633b)는, 예를 들어 1방향성 함수를 사용하여 챌린지 키로부터 인증 키를 생성한다.

비교회로(635a, 635b)는 2개의 인증 키가 일치하는가의 여부를 비교한다.

일시 키 생성회로(637a, 637b)는, 예를 들어 1방향성 함수를 이용하여 2개의 인증 키로부터 일시 키를 생성한다.

인증 키 생성회로(633a)와 인증 키 생성회로(633b)는, 예를 들어 동일한 알고리즘을 사용함으로써 동일한 챌린지 키에 대해 동일한 인증 키를 생성하는 것으로 한다.

일시 키 생성회로(637a)와 일시 키 생성회로(637b)는, 예를 들어 동일한 알고리즘을 사용함으로써 동일한 2개의 인증 키로부터 동일한 일시 키를 생성하는 것으로 한다.

다음에 도 15, 도 16을 참조하면서 키 공유의 절차에 대하여 설명한다.

우선 키 공유수단의 페이스 1에서는, 노드 2에서 챌린지 키 생성회로(631a)에 의해 챌린지 키(Challenge Key)(CK1)를 생성하고, 이것을 노드 #1에 전달한다.

다음에 노드 #2의 인증 키 생성회로(633a)와 노드 #2의 인증 키 생성회로(633b)의 각각에서 챌린지 키(CK1)에 의거해서 인증 키(key 1)(K1)를 생성하고, 또 노드 #1로부터 노드 #2에 생성한 인증 키(K1)를 전송한다.

그리고 노드 # 2에서, 비교회로(635a)에 의해 노드 #2와 노드 #1의 각각에서 생성된 2개의 인증 키(K1)를 비교한다. 만일 일치하면 다음의 페이스 2로 이행한다. 만일 일치하지 않으면 이상 종료가 된다.

다음에 페이스 2에서는, 노드 #1에서 챌린지 키 생성회로(631b)에 의해 챌린지 키(Challenge Key)(CK2)를 생성하고, 이것을 노드 #2에 전달한다.

다음에 노드 #1의 인증 키 생성회로(633b)와 노드 #2의 인증 키 생성회로(633a)의 각각에서, 챌린지 키(CK2)에 의거해서 인증 키(key 2)(K2)를 생성하고, 또 노드 #2로부터 노드 #1에 생성한 인증 키(K2)를 전송한다.

그리고 노드 #1에서, 비교회로(635b)에 의해 노드 #1과 노드 #2의 각각에서 생성된 2개의 인증 키(K2)를 비교한다. 만일 일치하면 다음의 페이스 3으로 이행한다. 만일 일치하지 않으면 이상 종료가 된다.

그리고 페이스 3에서는, 노드 #2의 일시 키 생성회로(637a)와 노드 #1의 일시 키 생성회로(637b)의 각각에서 인증키(K1)와 인증 키(K2)에 의거해서 일시 키(BUS Key) 즉 일시 키(Skt)를 생성한다.

여에 따라 노드 #1과 노드 #2 사이에서 안전하게 일시 키(Skt)가 공유화된다.

발명의 효과

상술한 바와 같이 본 발명의 실시예에 관한 부정 데이터 카피 방지장치 및 방법은 제1, 제2 또는 제3 실시예와 마찬가지 구성으로 한 외에, 마스터 키를 사용하지 않고 송신기기와 수신기기 사이에서 일시 키(Sk)를 안전하게 공유할 수 있도록 하였으므로, 제1, 제2 또는 제3 실시예와 마찬가지 효과가 얻어지는 외에, 기기간을 접속하는 케이블로부터 다른 기록매체에 기록하여 재이용하는 부정한 카피를 보다 한층 확실히

방지할 수가 있다.

그리고 본 발명은 상기 각 실시예에 한정되는 것이 아니라, 그 요지를 일탈하지 않은 범위에서 여러 가지로 변형할 수가 있다.

또 각 실시예에 기재한 방법은 컴퓨터로 실행시킬 수 있는 프로그램이며, 예를 들어 자기 디스크(플로피 디스크, 하드디스크 등), 광 디스크(CD-RAM, DVD 등), 반도체 메모리 등의 기억매체에 저장하거나, 또는 통신매체에 의해 전송하여 반포할 수도 있다. 본 장치를 실현하는 컴퓨터는 기억매체에 기록된 프로그램을 판독하고, 이 프로그램에 의해 동작이 제어됨으로써 상술한 처리를 실행한다. 또 컴퓨터는 소위 계산기뿐 아니라 디지털재생 기록기기 등의 모든 정보처리장치를 포함하는 것이다.

이상 상세히 설명한 바와 같이 본 발명에 의하면, 데이터 내의 카피를 관리하는 부분에 대한 부정자의 공격을 확실히 방어할 수 있는 부정 데이터 카피 방지장치 및 방법과 기록매체를 제공할 수가 있다.

또 본 발명에 의하면, 부정한 카피 데이터를 유효하게 재생시키지 못하도록 하는 부정 데이터 카피 방지장치 및 방법을 제공할 수가 있다.

그리고 본 발명에 의하면, 조직적인 카피관리를 실현할 수 있는 부정 데이터 카피 방지장치 및 방법을 제공할 수가 있다.

(57) 청구의 범위

청구항 1

디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지장치로서,

상기 디지털 데이터는 암호화된 데이터 본체와, 상기 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보를 가지며,

상기 카피관리 정보의 내용이 소정의 조건을 만족하고 있는가의 여부에 의거해서, 상기 디지털 데이터가 카피 허가인가의 여부를 판정하는 판정부와,

상기 판정부에 의해 상기 디지털 데이터가 카피 불허가이라고 판정된 경우에는, 상기 디지털 데이터의 유효한 카피 동작을 금지하는 금지 처리부를 구비하는 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 2

제1항에 있어서, 상기 데이터 본체를 암호화하기 위한 암호 키와 상기 카피관리 정보를 암호화하기 위한 암호 키는 상이한 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 3

제1항에 있어서, 상기 데이터 본체를 암호화하기 위한 암호 키와 상기 카피관리 정보를 암호화하기 위한 암호 키는 동일한 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 4

제1항에 있어서, 상기 카피관리 정보는 상기 디지털 데이터가 최초의 데이터로부터 몇회째의 카피인가를 나타내는 세대관리 정보와, 상기 디지털 데이터를 몇회 카피하였는가를 나타내는 카피회수관리 정보로 되며,

상기 판정부는 상기 세대관리 정보가 소정의 세대수가 되고, 상기 카피회수관리 정보가 소정의 카피회수가 되면 상기 디지털 데이터가 카피 불허가이라고 판정하는 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 5

제1항에 있어서, 상기 카피관리 정보는 상기 디지털 데이터가 최초의 데이터로부터 몇회째의 카피인가를 나타내는 세대관리 정보를 가지며, 상기 판정부는 상기 세대관리 정보가 소정의 세대수가 되면 카피 불허가이라고 판정하고, 상기 세대관리 정보는 3비트 이상의 데이터로 되는 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 6

제1항에 있어서, 상기 디지털 데이터를 송신기기와 수신기기 사이에서 전송할 때에, 상기 송신기기와 상기 수신기기간에 공유되는 일시 키를 암호 키 또는 복호 키로서 사용하여, 상기 디지털 데이터를 암호화 또는 복호화하는 암호화수단 또는 복호화수단을 더 구비하는 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 7

디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지장치로서,

상기 디지털 데이터는 암호화된 데이터 본체와, 상기 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보와, 상기 데이터 본체를 복호하기 위한 키정보를 가지며,

상기 카피관리 정보의 내용이 소정의 조건을 만족하고 있는가의 여부에 의거해서, 상기 디지털 데이터가 카피 허가인가의 여부를 판정하는 판정부와,

상기 판정부에 의해 상기 디지털 데이터가 카피 불허가이라고 판정된 경우에는, 상기 디지털 데이터 내의 상기 키정보를 변경하는 키 변경부를 구비하는 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 8

제7항에 있어서, 상기 데이터 본체를 암호화하기 위한 암호 키와 상기 카피관리 정보를 암호화하기 위한 암호 키는 상이한 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 9

제7항에 있어서, 상기 데이터 본체를 암호화하기 위한 암호 키와 상기 카피관리 정보를 암호화하기 위한 암호 키는 동일한 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 10

제7항에 있어서, 상기 카피관리 정보는 상기 디지털 데이터가 최초의 데이터로부터 몇회째의 카피인가를 나타내는 세대관리 정보와, 상기 디지털 데이터를 몇회 카피하였는가를 나타내는 카피회수관리 정보로 되며,

상기 판정부는 상기 세대관리 정보가 소정의 세대수가 되고, 상기 카피회수관리 정보가 소정의 카피회수가 되면 상기 디지털 데이터가 카피 불허가이라고 판정하는 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 11

제7항에 있어서, 상기 카피관리 정보는 상기 디지털 데이터가 최초의 데이터로부터 몇회째의 카피인가를 나타내는 세대관리 정보를 가지며, 상기 판정부는 상기 세대관리 정보가 소정의 세대수가 되면 카피 불허가이라고 판정하고, 상기 세대관리 정보는 3비트 이상의 데이터로 되는 것을 특징으로 하는 부정 데이터 카피 방지장치.

청구항 12

디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지방법으로서,

상기 디지털 데이터는 암호화된 데이터 본체와, 상기 데이터 본체의 카피 허가여 대해 관리하기 위한 암호화된 카피관리 정보와, 상기 데이터 본체를 복호하기 위한 키정보를 가지며,

상기 카피관리 정보의 내용이 소정의 조건을 만족하고 있는가의 여부에 의거해서, 상기 디지털 데이터가 카피 허가인가의 여부를 판정하는 판정공정과,

상기 판정공정에서 상기 디지털 데이터가 카피 불허가이라고 판정된 경우에는, 상기 디지털 데이터 내의 상기 키정보를 변경하는 키 변경공정을 구비하는 것을 특징으로 하는 부정 데이터 카피 방지방법.

청구항 13

디지털 데이터를 카피하는 기기에 사용되는 부정 데이터 카피 방지방법으로서,

상기 디지털 데이터가 최초의 데이터로부터 몇회째의 카피에 상당하는가를 나타내는 세대관리 정보와, 상기 디지털 데이터를 몇회 카피했는가를 나타내는 카피회수관리 정보로 된 카피관리 정보를 상기 디지털 데이터에 부가하는 부가공정과,

상기 세대관리 정보가 소정의 세대수가 되고, 상기 카피회수관리 정보가 소정의 카피회수가 되었을 때, 상기 디지털 데이터에 대한 카피 동작을 금지하는 금지공정을 구비하는 것을 특징으로 하는 부정 데이터 카피 방지방법.

청구항 14

컴퓨터에 의해 판독 가능한 데이터 구조가 기록된 기록매체로서,

상기 데이터 구조는

암호화된 데이터 본체와,

상기 데이터 본체의 카피 허가에 대해 관리하기 위한 암호화된 카피관리 정보와,

상기 데이터 본체를 복호하기 위한 제1 키정보와,

상기 카피관리 정보를 복호하기 위한 제2 키정보를 구비하는 것을 특징으로 하는 기록매체.

청구항 15

제14항에 있어서, 상기 데이터 본체를 암호화하기 위한 암호 키는 상기 카피관리 정보를 암호화하기 위한 암호 키와 상이한 것을 특징으로 하는 기록매체.

청구항 16

제14항에 있어서, 상기 데이터 본체를 암호화하기 위한 암호 키는 상기 카피관리 정보를 암호화하기 위한 암호 키와 동일한 것을 특징으로 하는 기록매체.

청구항 17

컴퓨터에 의해 판독 가능한 데이터 구조가 기록된 기록매체로서,

암호화된 데이터 본체와,

상기 데이터 본체를 복호하기 위한 데이터 암호 키가 상기 데이터 암호 키를 암호 키로 하여 암호화된 제1

키정보와,

상기 데이터 암호 키가 복수의 암호 키에 의해 각각 암호화된 복수의 제2 키정보와,

데이터 본체의 카피 허가에 대해 관리하기 위한 카피관리 정보가 상기 복수의 암호 키에 의해 각각 암호화된 복수의 제3 키정보를 구비하는 것을 특징으로 하는 기록매체.

청구항 18

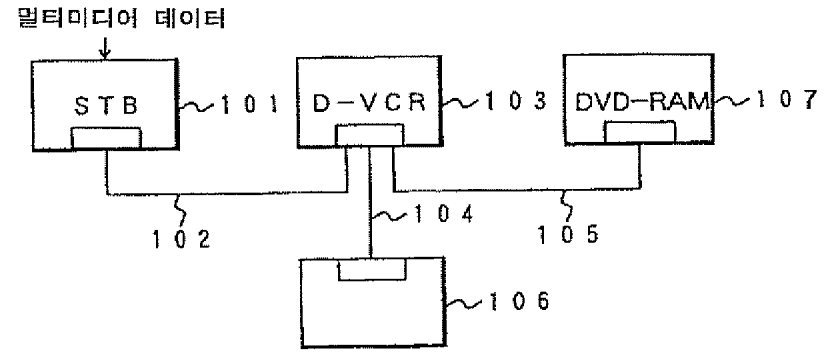
제17항에 있어서, 상기 데이터 암호 키와 상기 복수의 암호화 키는 상이한 것을 특징으로 하는 기록매체.

청구항 19

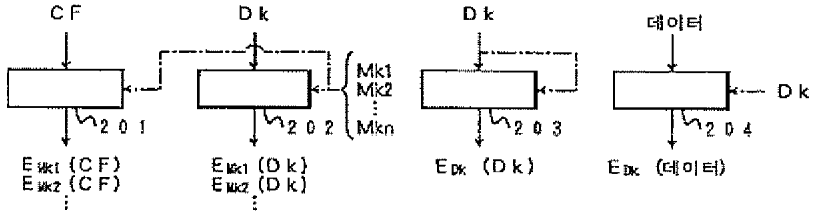
제17항에 있어서, 상기 데이터 암호 키와 상기 복수의 암호화 키는 동일한 것을 특징으로 하는 기록매체.

도면

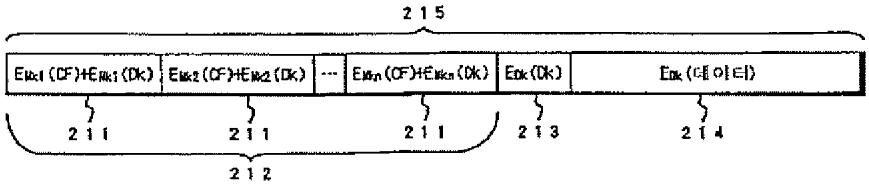
도면1



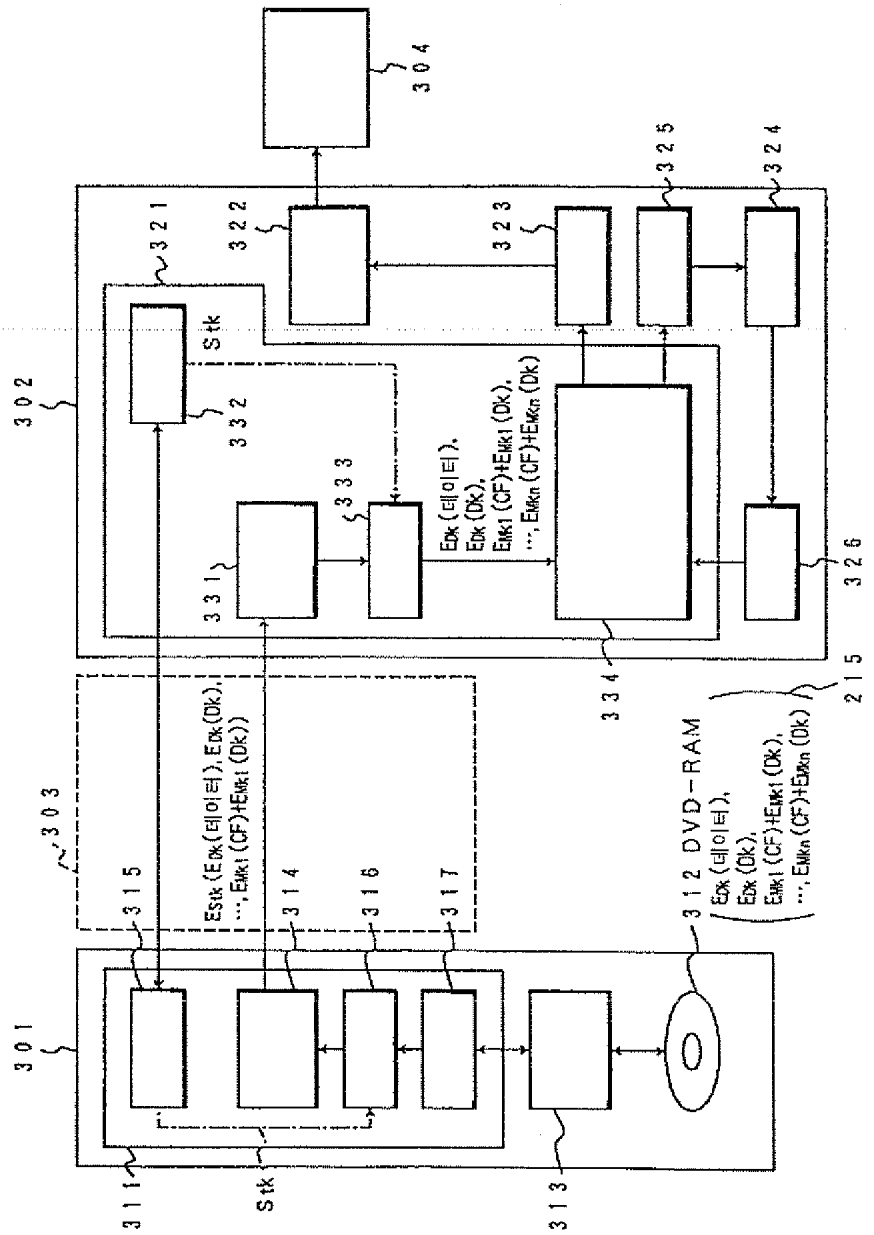
도면2



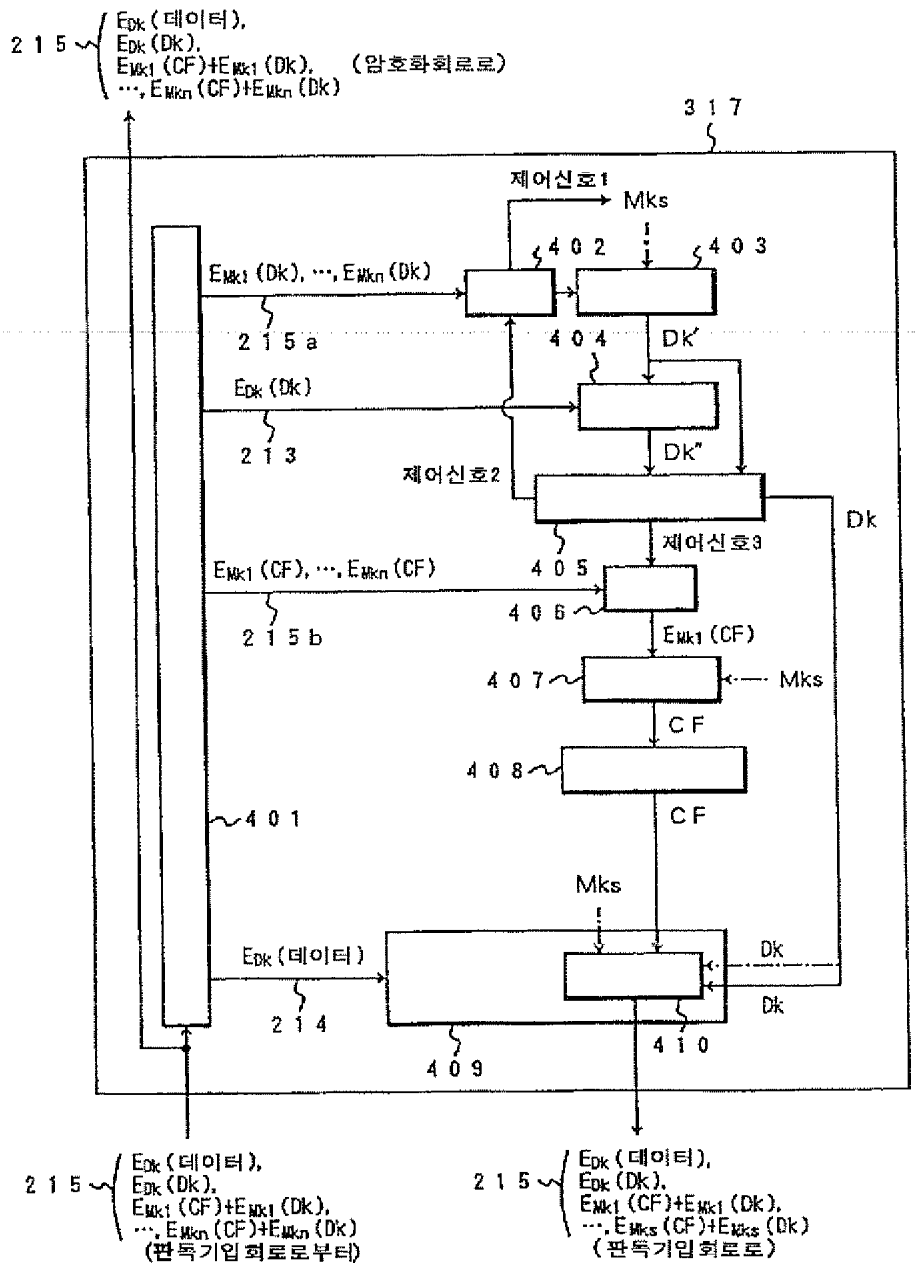
도면3



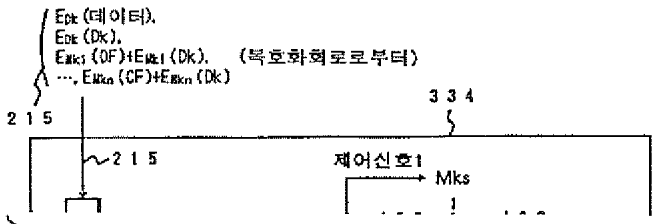
도면4


304
325
324
321
322
323
Stk
302
332
333
331
Edk (데이터키),
Edk (Dk),
EMk1 (CF)+EMk1 (Dk),
…, EMkn (CF)+EMkn (Dk)
326
334
215
303
Estk (Edk (데이터키), Edk (Dk),
…, EMk1 (CF)+EMk1 (Dk))
315
314
316
317
312 DVD-RAM
Edk (데이터키),
Edk (Dk),
EMk1 (CF)+EMk1 (Dk),
…, EMkn (CF)+EMkn (Dk)
301
311
Stk
313

도면5


215
EDk(데이터),
EDk(Dk),
EMk1(CF)+EMk1(Dk),
…, EMkn(CF)+EMkn(Dk)
(암호화회로로)
317
제어신호1
Mks
402
403
EMk1(Dk), …, EMkn(Dk)
215a
404
Dk'
EDk(Dk)
213
Dk"
제어신호2
Dk
제어신호3
405
EMk1(CF), …, EMkn(CF)
406
215b
EMk1(CF)
407
Mks
CF
408
401
CF
Mks
EDk(데이터)
Dk
214
Dk
409
410
215
EDk(데이터),
EDk(Dk),
EMk1(CF)+EMk1(Dk),
…, EMkn(CF)+EMkn(Dk)
(판독기입회로부터)
215
EDk(데이터),
EDk(Dk),
EMk1(CF)+EMk1(Dk),
…, EMks(CF)+EMks(Dk)
(판독기입회로로)

도면6


Epk (데이터),
Edk (Dk),
Ekk1 (DF)+Ekk1 (Dk), (복호화회로로부터)
…, Ekkn (DF)+Ekkn (Dk)
215
334
215
제어신호1
Mks

도면7

도면8

도면9

도면10

도면11

도면12a

도면12b

도면13

도면14

도면15

도면16